3GPP TSG SA WG3 Security — S3#32 **S3-040195**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title: Reply LS on WLAN authentication and authorization
Release: Rel-6
Work Item: WLAN Interworking

Source: SA3
To: CN1
Cc: SA2, CN4

Contact Person:
Name: **David Mariblanca**
Tel. Number: +34 646004736
E-mail Address: david.mariblanca@ericsson.com

1. Introduction

SA3 thanks CN1 for the received LS in order to align specifications. SA3 has investigated the assumptions and questions raised by CN1 in S3-040020 (N1-040163). The general comment is that CN1 working assumptions are mostly based on the support of EAP SIM and/or EAP AKA by the terminal to determine the method to use, but in fact it is the user's subscription that determines it.

2. Comments and conclusions

The following working assumptions being taken by CN1 are commented by SA3:

- *The 3GPP AAA server shall support both EAP SIM and EAP AKA based authentication as specified in the EAP SIM and EAP AKA specifications.*

Correct

- *The ME shall support both EAP SIM and EAP AKA based authentication, if the ME supports the ME-SIM interface.*

Yes, for R6+ MEs

- *By default, the EAP AKA method shall be used as primary authentication method in the EAP method negotiation.*

There is no default method, at least in the way suggested by the assumption above. The decision process of the method to start is as follows:

1. The WLAN UE will send an identity (whatever it is: permanent, pseudonym...) to the AAA server. In this identity is an IMSI, it will contain an indication of the EAP method to be used
2. If the AAA server recognizes the EAP method but not the user identity (for example an obsolete pseudonym), it will request a new identity using the EAP method indicated by the WLAN UE
3. If the AAA server recognizes the user identity (and hence the EAP method), it will fetch AVs from HSS. If they don't match the EAP method received (e.g. the EAP method recieved is EAP AKA and triplets are received from HSS), the user's subscription will prevail (in the previous example EAP SIM will be used).
4. If the user identity is not recognized, the AAA server will decide which method to use (there may exist a default method ONLY in this situation). If this default method does not match user's subscription (e.g. EAP AKA for a SIM user), the WLAN UE will respond a NACK to the AAA server and then the AAA will try with the other EAP method until a recognised identity is received.

Also, CN1 raised the following questions, for which SA3 provides some guidance:

- *If the ME supports the EAP AKA and EAP SIM methods and the 3GPP AAA server initiates authentication (i.e. EAP-Request/challenge) by means of the EAP SIM method rather than EAP AKA, what should be the ME behavior? Does the ME have to use the EAP AKA method as primary authentication method?*

The support of EAP AKA and/or EAP SIM in the ME does not determine the method to use, it is the user's subscription (to have a SIM or USIM card).

In any case, if the ME receives an EAP-Request proposing an unacceptable EAP method (i.e. not according to the user's subscription), then the ME shall respond with an EAP-Response/Nack indicating a method acceptable for the ME. In particular, the default EAP method policy of a Rel-6 ME shall only accept the EAP-AKA method if the subscription is based on a USIM, and EAP-SIM if the subscription is based on a SIM. However, it should be noted that this default policy may cause interoperability problems with pre-release 6 authentication servers that only support EAP-SIM authentication. Therefore, ME implementations may allow configuring an EAP method policy that allows EAP-SIM authentication even if a UICC with USIM has been inserted. The details and security aspects of ME policy configuration are for further study.

- *If 3GPP AAA server is aware that the ME supports the EAP AKA method, is the 3GPP AAA server mandated to always initiate the authentication (i.e. EAP-Request/challenge) by using the EAP AKA method, or is it allowed to use the EAP SIM method?*

The decision process is explained above. The ME shall not indicate the method(s) supported, but the method compatible with the smart card (SIM or USIM) contained, which additionally needs to be supported by the ME. Hence, the default EAP method policy of a Rel-6 3GPP AAA server shall not accept EAP-SIM for USIM subscribers. However, as such a policy may cause interoperability problems with pre-release 6 ME implementations that do not support EAP-AKA, the 3GPP AAA server may be support configuring an EAP method policy that accepts EAP-SIM authentication for USIM subscribers. This configuration option may be used, if many USIM subscribers are expected to use pre-release 6 ME implementations that do not support EAP AKA. The details and security aspects of AAA server policy configuration are for further study.

4. Actions:

To CN1 group.

SA3 kindly asks CN1 to consider the answers provided above when specifying the EAP method policies.

3. Date of Next TSG-SA3 Meetings:

SA3#33	11th – 14th May 2004	Beijing, China
SA3#34	06th – 09th July 2004	TBD (North American Friends)